The Impact of Going Dark: Implications of Service and Device Providers Failing to Keep or Provide Records for Criminal Investigations

Christopher A. Williams

Abstract

The playing field for today's criminal is less of a dark alley and more of a Starbuck's with Wi-Fi. Technology aided or enabled crime is a significant threat facing law enforcement. Technology by its very nature stores data. That data can prove useful to detect, arrest, and prosecute criminals. Data can be stored in many places, but most notably it is stored in digital storage devices (cell phones, tablets, smart watches, computers, and cameras) and with digital service or social media providers. The "going dark" problem outlines device manufacturers and digital service providers that do not allow for access to this data to further an investigation. By recognizing this problem, law enforcement can work to keep pace with the changing landscape of technology and crime trends.

Introduction

The ever increasing popularity of personal electronic devices and the amount of personal data contained therein has elevated consumer concerns for protecting this data. The impact of "going dark" on criminal investigations is inherently difficult to measure in that there is no way of knowing what information may or may not have been available on the device or service provider. Law enforcement agencies across the country are reporting that increasing security which protects digital storage devices from unauthorized access also presents a challenge to law enforcement attempting to legally access the data to further a criminal investigation. This issue has garnered media attention with several high profile criminal investigations which were purportedly hindered by law enforcement's inability to access the data contained on the digital storage device. Additionally, many internet service and social media service providers are choosing to not retain records which present an additional challenge to law enforcement. This research seeks to identify the scope and severity of the problem impacting law enforcement in Florida.

Literature Review

Device encryption:

The advent of mobile internet enabled smartphones has transformed the way people live, work, play, and commit criminal acts. With one touch, the criminal or the criminal investigator is connected to global network enabling crime fighters with a major tool, and also a major challenge. Just as criminals leave footprints, DNA, and fingerprints at a traditional crime scene, they also leave a digital fingerprint that is just as, if not more capable of proving a case. Access to this digital information enables law enforcement to solve crime and protect the public. One challenge that results from increased connectivity is that criminals have easier access to data and communications. The more pressing challenge is law enforcement's inability to intercept live data as well as access and/or review saved data. Both live and stored data are being encrypted by device and service providers alike. In short, encrypted data is locked so that only people with access can obtain access. (Cunningham, 2016)

The purpose of encrypting data is to protect it from unauthorized access. FBI Director James Comey warned of "public safety and national security risks" posed by terrorists utilizing encryption. Director Comey sought for U.S. based tech companies to provide a law enforcement "backdoor" to ensure information is accessible when required. Opponent organizations, such as the Electronic Frontier Foundation, argue that government and nefarious cryptologists operate in the same digital environment and it's not possible to allow access to law enforcement while simultaneously ensuring security against attacks. Opponents also argue that it is essentially a slippery slope when it comes to who "backdoor" access is provided to, making a note of the difference between the U.S. and China governments. (Cohn, 2015)

Encryption, or what law enforcement commonly call "going dark," is a double-edged sword. It does, in fact, safeguard personal information from nefarious access. That same safeguard protects criminals from disclosing potentially key evidence of their criminal activity. The latter safeguard has real-world consequences that as of recent were highlighted by high-profile mass shootings in the U.S. and abroad. Technology manufacturers that do not comply with court-ordered surveillance requirements impact both real-time and saved data. The absence of either type of data can hinder prosecution at best, or can prevent the early detection of a significant threat to public safety at worst. (Cunningham, 2016)

In looking at implications of device encryption and potentially allowing "backdoor access" from a broad perspective, it should be noted that public safety is only one concern. Mobile smartphones are today's key to global commerce. Online shopping, banking, information exchange, business dealings, and a host of activities are accomplished through the use of encrypted devices. In the event a digital "backdoor" is created, it is likely that bad actors will specifically target the same access provided to law enforcement. This "backdoor" could open U.S. based mobile devices up to espionage and puts the U.S. market at a global disadvantage. (Cohn, 2015)

Some find that there is room for compromise as it relates to individual right to privacy versus the government's need to conduct investigations. A bipartisan group from the U.S. House of Representatives found that law makers should "foster cooperation between the law enforcement community and technology companies." The group further stated that "any measure that weakens encryption works against the national interest." (Curran, 2016)

Service provider retention:

Evidence of cyber-crime can generally be found in two separate yet equally important storage locations. First, the physical device used to access communication networks such as a computer, tablet, or smartphone. As previously referenced, encryption presents a challenge to law enforcement with regards to obtaining data from the device itself. (Cunningham, 2016) The second evidence location is the service provider. Service providers include cellular service provers, internet service providers, computer program and application providers, and (in some cases) device providers.

Service providers, in a broad sense, can provide investigators with user subscriber records, historical usage records, historical communication records, and in some cases can enable the live intercept of communication. There are two challenges that have become very prominent in the criminal justice area with regards to service providers aiding in criminal investigations: ability to comply and desire to comply.

First, there are no global standards with regards to what records are kept for storage, how long those records are preserved, and the legal process required to access those records. United States based companies are bound by the Communications Assistance for Law Enforcement Act (CALEA) passed in 1994. In summary, the law requires communications service providers to allow for intercept of communication via court-order and has minimum standards of data retention. (Brown, 2015) CALEA only applies to the U.S. which can make global based cyber-crime investigations more challenging. The ambiguity among service providers is compounded by the global, multi-jurisdictional environment in which cyber-crime is investigated. (Brown, 2015) The lack of standards in the service provider arena makes that industry's ability to comply hit and miss. Some provider's business model (such as Google) requires the preservation of copious amounts of data relating to their customers. Other providers choose not to preserve records. In some cases law enforcement seeks out records from a company who does not have the ability to comply with the request. (Brown, 2015) One factor impacting the ability to comply is cost. Storing records (data) costs money. In short, the more records that are stored, the higher the cost for the provider. The cost for records is driven up sharply when record access is needed in real-time, such as a Title III intercept. There are some service providers who do not have the financial means to comply with such a request, even if the provider had the desire to assist in the investigation. (Brown, 2015)

Second to ability is the service provider industry's desire to comply with a legal request from law enforcement. In some cases, a service provider's business model is built upon the presumption of privacy and/or anonymity. Service providers such as this are reluctant to allow law enforcement access to basic user information which can have a tremendous impact on investigations. (Brown, 2015)

Legal hurdles:

The investigation of cyber-related criminal activity is inherently technically complex and presents challenges for law enforcement and the courts in many respects. The legal system itself has and continues to face challenges in adapting to crime trends. The first legal challenge in the investigation and prosecution is defining cyber-crime. There is a general lack of consistency in the criminal justice system when it comes to the definition of cyber-crime. (Brown, 2015) High technology crime, computer crime, e-crime, technology-enabled crime, and cyber-crime are terms that are all used synonymously. (Brown, 2015) Additionally, activity associated with cyber-crime must specifically be criminal in nature (there must be a law prohibiting the specific conduct) in order for law enforcement to become involved. With the ever-changing landscape of technology, the criminal justice system is, in most cases, lagging behind in legal updates addressing new trends (Brown, 2015). In broad terms cyber-crime must meet the following elements: the conduct is facilitated by technology, the conduct is motivated by intent to harm a person or organization, the harm causes interference or damage to a person or organization, and the conduct is criminalized in the jurisdiction in question. (Brown, 2015) It is difficult, at best, to address cyber-crime in specific terms in the law. Instead, laws must be tailored to address cyber-crime concerns from a broad perspective to lessen the impact of dynamically changing technology on the legal system. (Brown, 2015)

Evidence of cyber-crime is rarely found through traditional means such as physical surveillance, witness statements, and latent print analysis. While each of the aforementioned investigative techniques could be utilized in a cyber-crime investigation, most evidence of cyber-crime is stored in data storage devices such as hard drives, cloud storage drives, USB drives, and records from internet service providers. (Brown, 2015) These pieces of evidence are critical to the successful prosecution in a cyber-crime investigation. A significant challenge to obtaining evidence in a cyber-crime investigation is the multi-nation jurisdiction that often involves cyber-crimes. The World Wide Web, as the name implies, means that evidence (data in this case) is usually physically stored all over the world. (Brown, 2015) The location of the stored data can present challenges to an investigation with respect to jurisdiction and differing laws addressing cyber-crime. While there are legal provisions in place to address criminal acts in foreign jurisdictions, the application of these laws are ineffective. (Brown, 2015)

In addition to the above challenges, there is no consensus among service providers with regards to what legal process is required to obtain information in a criminal investigation. While some require a subpoena, others may require a court-order or search warrant. (Brown, 2015) There is significant political disagreement globally with regards to a service provider's responsibility to keep records, as well as the government's ability to access them. Privacy rights proponents argue that private life and personal data are to be protected. Globally, there is agreement that there are times the government should have access to data or records that are strictly necessary. The subjective argument is based on what is considered necessary, and what is considered personal/ private data. (Brown, 2015)

The newest legal challenge to impact the criminal justice community with respect to cyber-crime is the advent of cloud-based storage and computing. Laws are, by design, locally and geographically based whereas cloud technology is intrinsically global in nature. (Brown, 2015) The physical location for a cloud storage device may be spread out across multiple jurisdictions, countries, and in many cases continents. Navigating the different laws associated with multiple jurisdictions can be challenging, at best.

While there is significant disagreement over encryption and back door government access, it should be noted that if laws were changed in the U.S. to allow for government access, the laws would apply only to U.S. based companies. (Curran, 2016) Encryption advocates argue that the impact of a pro law enforcement encryption law would have profound impact on the security of U.S. based devices and providers, but little to no impact on a criminal ability to use overseas based encryption means to conceal their illicit activities. (Curran, 2016)

Impact to the State of Florida:

Starting in late 2014, the Florida Department of Law Enforcement (FDLE) began tracking device and service provider issues with regards to legal process compliance in criminal investigations. The FDLE utilized a collection tool developed by the National Domestic Communications Assistance Center (NDCAC) and tracked in the areas of device forensics, provider records requests, and wiretap (live data) requests. (FDLE, 2019) Information was collected from local and state law enforcement agencies. Participation by law enforcement agencies with the FDLE was voluntary, so it is likely the number of reports noted by the FDLE is lower than the actual numbers for the State of Florida.

From late 2014 through January 2019, the FDLE logged a total of 218 cases where law enforcement was unable to fully obtain data from an electronic storage device (in most instances a smartphone). The FDLE noted 44 Android platform devices and 46 iOS (Apple) platform devices were unable to be analyzed. An additional 128 devices were unable to be analyzed but no device manufacturers were noted. (FDLE, 2019)

From late 2014 through January 2019, the FDLE logged a total of two cases where law enforcement was unable to fully obtain data from a service provider. In one case, records were not preserved or available and the other case records were provided in an encrypted format the company refused to decrypt. There were no reported issues for live data intercept according to the FDLE.

Based on the FDLE statistics, cases impacted include but are not limited to: drug offenses, sexual battery, larceny, robbery, weapons offenses, public corruption, network intrusion, burglary, and homicide.

Methods

The purpose of this research was to identify whether or not Florida law enforcement agencies have experienced an impact on investigations as a result of being unable to recover encrypted data from digital storage devices, or being unable to recover data from digital service providers.

Data was gathered through surveys provided to multiple law enforcement agencies throughout the state of Florida via the Internet Crimes against Children distribution list (148 members) and the Florida Department of Law Enforcement internal Cyber High Tech Crime distribution list (80 members). Survey questions were designed to determine if law enforcement agencies had been unable to recover data from an encrypted digital storage device or digital service provider. Questions also asked participants about specific operating systems such as Android and iOS as well as recovery of data from social media platforms. Questions also sought to determine if the inability to recover data had a negative impact on the ability to prosecute the case.

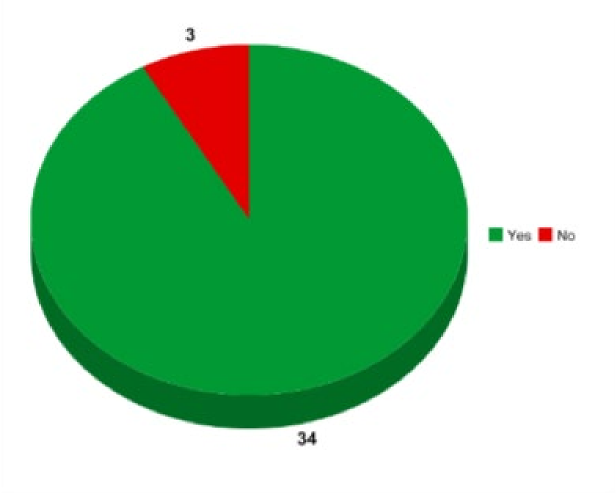
The survey was disseminated anonymously to encourage honest feedback as well as simplify the survey process. A weakness in the data collected is that it fails to capture information from every law enforcement agency who deals with processing digital evidence.

Results

The survey was sent to 228 law enforcement officers and analysts engaged in cyber-crime investigations in the state of Florida. I received 37 responses, for a response rate of 16.2%. Six questions received a 100% response. Four questions received a 97% response (one respondent did not answer). All questions were asked with the qualifier “in the past five years” to ensure responses were aligned with current trends.

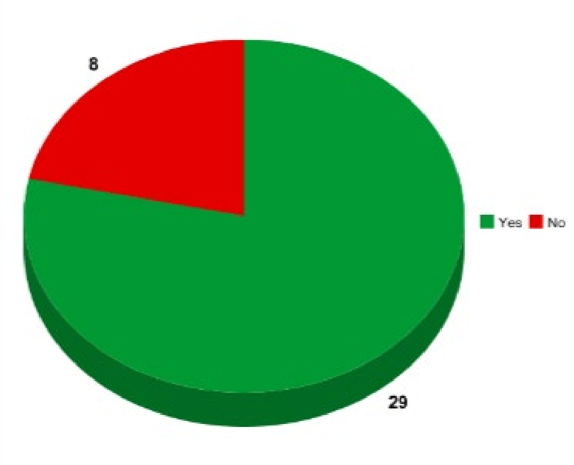
The first question on the survey asked respondents about the inability to obtain data from a locked or encrypted digital storage device. In total, 91.89% (34) of those surveyed noted they have been unable to recover encrypted or locked data from devices believed to contain evidence in a criminal investigation. All respondent’s answered this question.

Question One



The second question on the survey asked respondents about the inability to obtain data from a digital service provider. In total, 78.38% (29) of those surveyed noted they have been unable to recover data from a digital service provider believed to contain evidence in a criminal investigation. All respondent's answered this question.

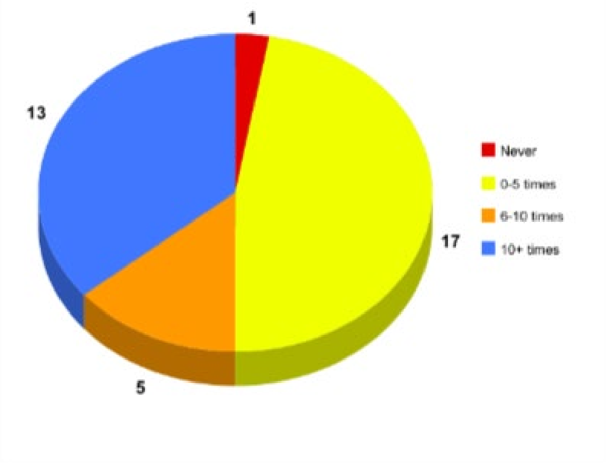
Question Two



Questions three, four, and five on the survey asked respondents about the inability to obtain data from specific locked or encrypted digital storage devices and the frequency thereof. The survey categorized answers into four categories: never, 0-5 times, 6-10 times, and 10+ times.

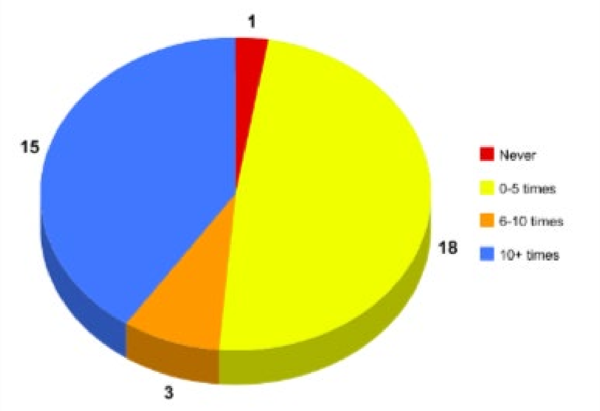
Question three asked about devices with Android operating systems and the inability to obtain data from those types of devices and the frequency thereof. The survey revealed 47.22% (17) of those surveyed noted they have been unable to recover encrypted or locked data from an Android device believed to contain evidence in a criminal investigation up to five times in the past five years. Additionally, 13.89% (5) of those surveyed noted the frequency 6 to 10 times, 36.11% (13) of those surveyed noted the frequency over ten times in the past five years, and 2.78% (1) of those surveyed had never been unable to recover data from an Android operating system in the past five years. One respondent did not answer this question.

Question Three



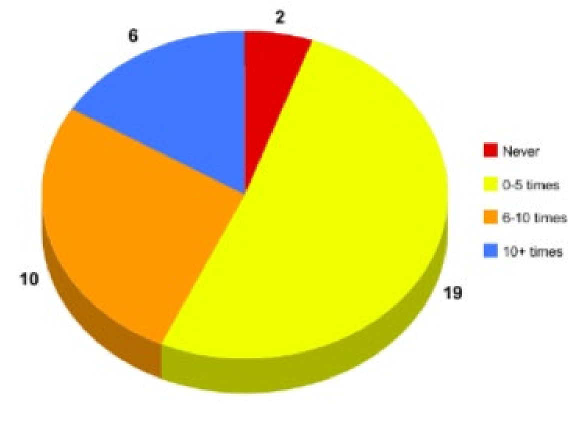
Question four asked about devices with iOS operating systems and the inability to obtain data from those types of devices and the frequency thereof. The survey revealed 48.65% (18) of those surveyed noted they have been unable to recover encrypted or locked data from an iOS device believed to contain evidence in a criminal investigation up to five times in the past five years. Additionally, 8.11% (3) of those surveyed noted the frequency 6 to 10 times, 40.54% (15) of those surveyed noted the frequency over ten times in the past five years, and 2.7% (1) of those surveyed had never been unable to recover data from an iOS operating system in the past five years. All respondent's answered this question.

Question Four



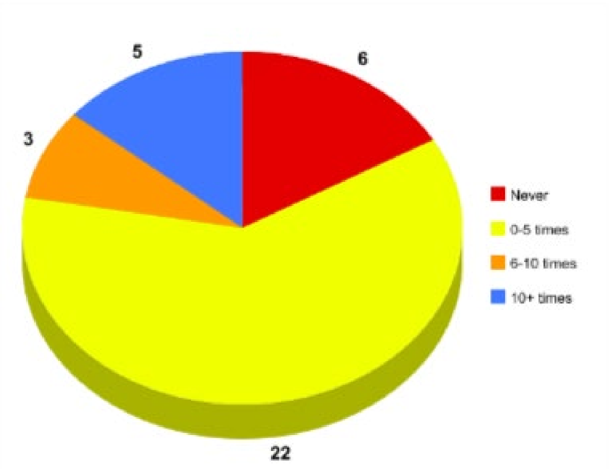
Question five asked about devices with non- Android or iOS operating systems and the inability to obtain data from those types of devices and the frequency thereof. The survey revealed 51.35% (19) of those surveyed noted they have been unable to recover encrypted or locked data from a non- Android or iOS device believed to contain evidence in a criminal investigation up to five times in the past five years. Additionally, 27.03% (6) of those surveyed noted the frequency 6 to 10 times, 16.22% (6) of those surveyed noted the frequency over ten times in the past five years, and 5.41% (2) of those surveyed had never been unable to recover data from a non-Android or iOS operating system in the past five years. All respondent's answered this question.

Question Five



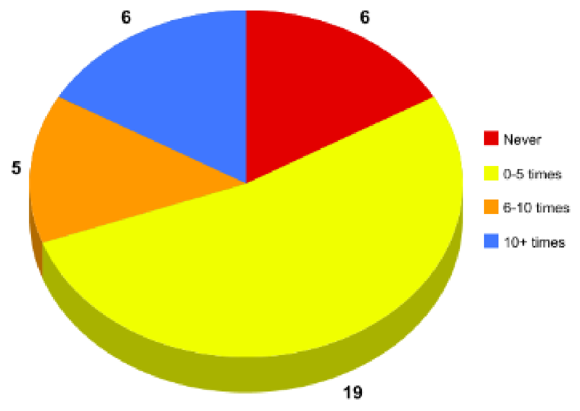
Question six asked about the respondent's inability to recover data from an internet service provider and the frequency thereof. The survey revealed 61.11% (22) of those surveyed noted they have been unable to recover data from an internet service provider up to five times in the past five years. Additionally, 8.33% (3) of those surveyed noted the frequency 6 to 10 times, 13.89% (5) of those surveyed noted the frequency over ten times in the past five years, and 16.67% (6) of those surveyed had always successfully recovered data from an internet service provider in the past five years. One respondent did not answer this question. All respondent's answered this question.

Question Six



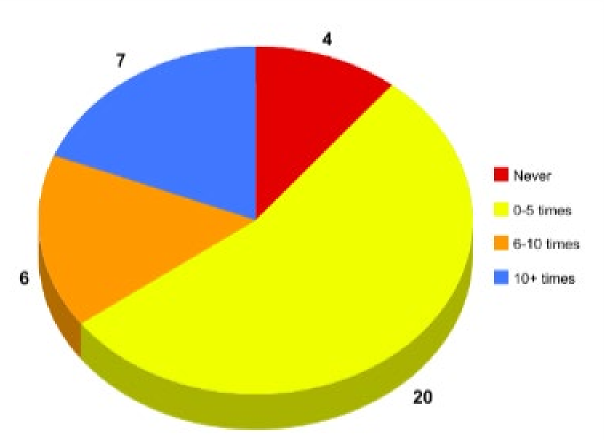
Question seven asked about the respondent's inability to recover data from a social media provider and the frequency thereof. The survey revealed 52.79% (19) of those surveyed noted they have been unable to recover data from an internet service provider up to five times in the past five years. Additionally, 13.89% (5) of those surveyed noted the frequency 6 to 10 times, 16.67% (6) of those surveyed noted the frequency over ten times in the past five years, and 16.67% (6) of those surveyed had always successfully recovered data from a social media provider in the past five years. One respondent did not answer this question.

Question Seven



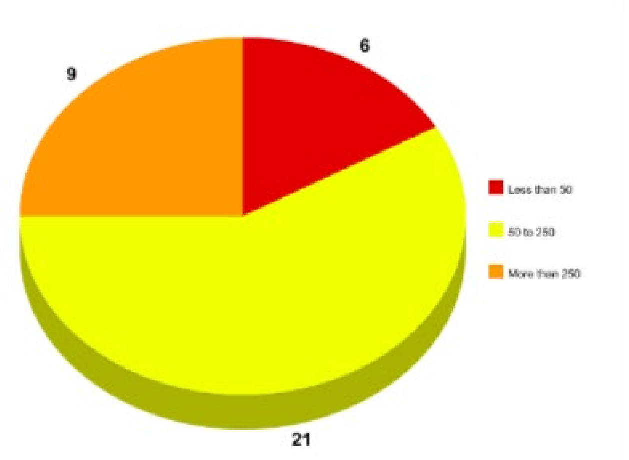
Question eight asked about the respondent’s experience relating to a negative impact on the criminal prosecution of a case as a result of being unable to recover data from a digital storage device or an internet service provider and the frequency thereof. The survey revealed 54.05% (20) of those surveyed noted they had a negative case impact up to five times in the past five years. Additionally, 16.22% (6) of those surveyed noted the frequency 6 to 10 times, 18.92% (7) of those surveyed noted the frequency over ten times in the past five years, and 10.81% (4) of those surveyed had a negative case impact in the past five years. All respondent’s answered this question.

Question Eight



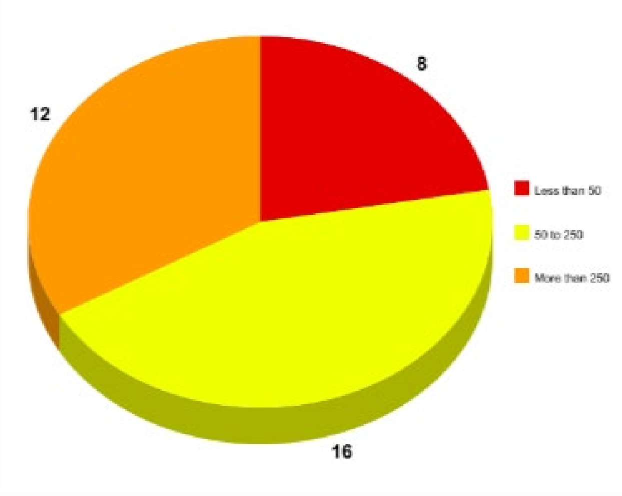
Question nine asked about the volume of requests the respondent’s agency made for records from any digital service provider in the past five years. The survey revealed 16.67% (6) of those surveyed noted they have made less than 50 requests for records in the past five years. Additionally, 58.33% (21) of those surveyed noted they have made 50 to 250 requests for records in the past five years and 25% (9) of those surveyed noted they have made over 250 requests for records in the past five years. One respondent did not answer this question.

Question Nine



Question ten asked about the volume of attempted and completed data recoveries the respondent’s agency made in the past five years. The survey revealed 22.22% (8) of those surveyed noted they have made less than 50 attempts or completed data recoveries in the past five years. Additionally, 44.44% (16) of those surveyed noted they have made 50 to 250 attempts or completed data recoveries in the past five years and 33.33% (12) of those surveyed noted they have made over 250 attempts or completed data recoveries in the past five years. One respondent did not answer this question.

Question Ten



Discussion

The result of the survey confirms what the existing literature details. The results provide additional insight into the service provider arena, which appears to be an increasing source of information for criminal investigations. Based on the results, respondents also represent a variety of involvement in investigations involving devices and providers. Some respondents had over 250 cases in the past five years and some fewer than 50.

The survey noted the volume of cases worked with regard to devices and service provider data requests. The results were similar. Between 16% and 22% of those surveyed had worked less than 50 cases in the past five years. Most respondents (44% to 58) had worked between 50 and 250 cases. Between 25% and 33% of those surveyed had worked over 250 cases in the past five years. The survey confirms that law enforcement is working a significant number of investigations involving digital storage devices and service providers.

Based on the survey results, an overwhelming 91.89% of those surveyed have been unable to recover data from encrypted or locked devices. This confirms that encryption is still an issue impacting law enforcement investigations in Florida. The survey also highlighted problems with digital service providers that were not as clearly defined in the literature review. 78.38% of those surveyed have had problems recovering data from digital service providers placing it a close second place to being unable to recover data from the devices themselves. This statistic has not been tracked from a statewide perspective and poses a significant gap to law enforcement.

In review of Android; iOS; and other devices and the inability to recover data, Android and iOS device survey results were very similar. Almost half of the respondents had problems obtaining data up to five times, and between 36 % and 40% had problems over ten times. With respect to non-Android and non-iOS devices, the responses indicate slightly over half had problems up to five times, and over 16% had problems over ten times.

The survey provided additional insight into digital service and social media providers. The survey results were similar for both. Over 16% of those surveyed have never had an issue with this. Between 52% and 61% had issues obtaining records from digital service or social media providers up to 5 times. With the increase in popularity of social media, the geo location of the servers running those platforms (some are overseas), and the criminal element adapting and exploiting new technology, I anticipate the frequency of these issues will rise.

The key question in this survey was the impact the above has had on the criminal prosecution of cases. Just over 10% of those surveyed have not had an impact meaning that almost 90% have had an impact. The majority of respondents (58.33%) had faced a negative impact up to five times. Unexpectedly, the survey noted that almost 19% had experienced a negative case impact over ten times. In summary, the inability to recover data from devices and service providers has had a significant impact on law enforcement and the ability to prosecute cases successfully.

Recommendations

The survey results indicate and confirm existing literature that notes digital device encryption impacts Florida law enforcement investigations. Additionally, the survey indicates that digital service and social media providers failing to provide data also impact investigations.

Technology is evolving faster today than at any point in history. And as such, law enforcement has and will continue to be (at best) one step behind technology advancement. There are two separate yet equally important areas for improvement to combat the “going dark” problem.

First, law enforcement cannot wait on new laws to be passed that require both device manufacturers and service providers to allow judicial reviewed access to data in furtherance of a criminal investigation. Law enforcement leadership should always seek to encourage the development of and deploy the most up-to-date software and hardware solutions that allow for access to digital storage devices allowed by the court. While this typically does not impact the service provider arena, it significantly impacts law enforcement’s ability to search devices.

Second, law enforcement leadership should lobby for changes to existing laws to account for the significant change in technology. Laws like the Communications Assistance for Law Enforcement Act (CALEA) passed in 1994 are woefully outdated. The intent of the legislature in 1994 was to require companies to provide court-ordered access to data and require a minimum records retention period for telephone communications. While this law does still impact some of the digital service providers, it is significantly outdated and allows more loop holes than not with regards to today’s digital services.

From a state perspective, Florida State Statute 934.03 addresses the intercept of electronic communication, but it does not go far enough in identifying electronic service and social media service providers with regards to records retention as CALEA does with phone companies. An amended law requiring all electronic service providers and social media providers to preserve and maintain records for a period of time would enable law enforcement to have judicially reviewed access to critical information to further criminal investigations.

The skyrocketing prevalence of digital devices and the amount of data stored both on the device and with the service providers is incalculably high and is increasing by the minute. While the intent of the technology sector is not to enable the criminal element, many of the technologies developed for good can be exploited for evil. As such, law enforcement must adapt and proactively seek to make an impact on the "going dark" problem to ensure that the criminal element's ability to exploit technology is never outweighed by law enforcement's ability to detect, preserve, and collect digital evidence.

Assistant Special Agent in Charge (ASAC) Chris Williams joined the Florida Department of Law Enforcement (FDLE) in 2008 as a special agent assigned to the Fort Myers Regional Operations Center. Later that year he transferred to the Pensacola Regional Operations Center (PROC). He has served on the PROC Cyber/High-Tech Crime and Major Case squads. In 2015, Chris was appointed acting Special Agent Supervisor (SAS), and later promoted to the role, where he supervised the Major Case, Organized Crime and Counterterrorism squads. Prior to joining FDLE, Chris served as a deputy sheriff and detective with the Santa Rosa County Sheriff's Office with assignments in the Patrol, Traffic/DUI Enforcement and Criminal Investigations/Narcotics divisions. Chris earned a Bachelor's Degree in Criminal Justice from the University of West Florida.

References

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9*(1), 55-119. Retrieved from https://login.proxy.lib.fsu.edu/login?url=https://search.proquest.com/docview/1707836020?accountid=4840

Cohn, C. (2015, Dec 23). The debate over encryption: The backdoor is a trapdoor; Giving the government keys to encrypted software will make Americans less safe. *Wall Street Journal (Online)* Retrieved from https://login.proxy.lib.fsu.edu/login?url=https://search.proquest.com/docview/1751302564?accountid=4840

Cunningham, T.M. (2015, January). Presidential focus: Going dark and the challenges of gathering electronic evidence. *The Police Chief, 83*(6).

Curran, J. (2016). Congressional report on encryption urges search for ‘common ground’. *Cybersecurity Policy Report, 1*. Retrieved from https://login.proxy.lib.fsu.edu/login?url=https://search.proquest.com/docview/1854199870?accountid=4840

State of Florida. Florida Department of Law Enforcement. (2019). NDCAC statistics collection tool.

Appendix A

Survey

The impact of going dark: Implications of service and device providers failing to keep or provide records for criminal investigations

1.) Has your agency been unable to recover data from an encrypted or locked digital storage device which is believed to contain evidence in a criminal investigation in the past five years?

    Yes
    No

2.) Has your agency been unable to recover data from a digital service provider which is believed to contain evidence in a criminal investigation in the past five years?

    Yes
    No

3.) How many times has your agency been unable to recover data from an Android operating system based digital storage device in the past five years?

    Never
    0-5 times
    6-10 times
    10+ times

4.) How many times has your agency has been unable to recover data from an iOS operating system based digital storage device in the past five years?

    Never
    0-5 times
    6-10 times
    10+ times

5.) How many times has your agency has been unable to recover data from a non-Android or iOS operating system based digital storage device in the past five years?

    Never
    0-5 times
    6-10 times
    10+ times

6.) How many times has your agency been unable to recover data from an internet service provider in the past five years?

Never
0-5 times
6-10 times
10+ times

7.) How many times has your agency has been unable to recover data from an social media service provider in the past five years?

Never
0-5 times
6-10 times
10+ times

8.) How many times has your agency experienced a negative impact on the criminal prosecution of a case as a result of the inability to recover data from a digital storage device or a digital service provider in the past five years?

Never
0-5 times
6-10 times
10+ times

9.) How many times has your agency conducted requests for digital service provider information or records in the past five years?

Less than 50
50 to 250
More than 250

10.) How many times has your agency conducted or attempted successful digital storage device data recoveries in the past five years?

Less than 50
50 to 250
More than 250